OUTLINE OF RESEARCH WORK ENTITLED

Algebraic Codes Over Finite Fields And Finite Rings

Submitted to

Swami Ramanand Teerth Marathwada University
Nanded-431606, Maharashtra State, India

For Registration of (Ph.D) Doctor of Philosophy in Mathematics

Research Student

Mrs. Somaiyah Aqeel Ali Abdulsattar

Under the Guidance of

Dr. Arunkumar R. Patil
Department of Mathematics,
SGGS Institute of Engineering and Technology,
Swami Ramanand Teerth Marathwada University,
Nanded-431606, Maharashtra, India.

August 21, 2021

Introduction:
Linear codes over finite fields and finite rings are an emerging area of reserach and lies at the crossroad of abstract algebra and coding theory. I would like to pursue my reserach to study some imporatnt class of linear codes over these finite alphabets-finite fields and finite rings. This could include cyclic codes and their furthur generalizations such as constacyclic codes and nega cyclic codes, codes defined from algebraic curves, codes from commutative and non commutative rings. Study of different parameters, bounds , generator and parity check matrices using algebraic and combinatirial concepts is a great attraction to me and that is why I have chosen this field of research. Decoding techniques of some of these codes, construction of new codes from available codes through concatenation is also my interest for PhD.

1. **Review of Literature and development in the subject**

   Coding Theory became the subject of mathematical interets due to the landmark paper, *A Mathematical Theory of Communication*, by Shannon [5] in the year 1949 and in subsequent years by Hamming [4]. In coding theroy an electronic information could be transmitted through a noisy channel where an error is likely to happen. The message is sent in a string of binary digits 0's and 1's which are the elements of binary field $\mathbb{F}_2 = \{0, 1\}$. So a natural question arises what if the field $\mathbb{F}_2$ is replaced by any finite field $\mathbb{F}_q$ (where q power of any prime) or any finite ring R. These alphabets have a great algebraic structure and their various properties can be a rich source to construct various useful codes. So, this leads the attraction of many mathematicians towrads algebraic coding theory. Now a days coding theory has become the core area of reserach in pure mathematics. It has also various connections to combinatorics, graph theory, lattice theory, algebraic geometry, toplogy, etc.

   Since its inception a lot of progress is done in this area. various codes have been studied and applied from the use of sending the signal from Mars to earth to the data storage and compression, AI, Machine learning, etc. A very special class of linear codes called cyclic codes is studied by many reserachers due to its beutiful connections to algebraic structures.

   Let $\mathbb{F}_q$ be a finite field with q elements where q is a power of prime p and $\mathbb{F}_q^n$ be the n dimensional vector space over $\mathbb{F}_q$. Then an $[n, k]_q$- linear code C is a k dimensional subspace of $\mathbb{F}_q^n$. The vectors $(c_1, c_2, \cdots, c_n) \in C$ are called as codewords. The parameters n and k denote the length and dimension of C. The number of non zero entries in a codeword x of C is called the Hamming weight or Hamming norm and is denoted by $\|x\|$. The $\min\{\|x\| : x \in C\}$ is called minimum Hamming weight or minimum weight and is denoted by $d(C)$ or d if the context is clear.

   These parameters n, k, d determine how best is a given linear code. That means the eroor detection and error correction capability of these codes is determined by these parameters. So, naturally there are various bounds on linear codes such as: Singleton bound, Gilbert Varshamov Bound, Griesmer bound, etc. A code that achieve so called Singleton bound is called Maximum Distance Seperable (MDS) codes.

   There are various cyclic codes such as BCH codes, Reed Solomon Codes, which have been used due to their error detection and correction cpapbilities [12, 15].

   A linear code C is said to be cyclic if whenevr $(c_0, c_1, \cdots, c_{n-1})$ is in C, then its first cyclic shift $(c_{n-1}, c_0, \cdots, c_{n-2})$ is also in C. This property can naturalll be connected to the elegant

characterization of cyclic codes as ideals generated by a polynomial $f(x)$ of degree n in a polynomial ring $\mathbb{F}_q[x]$. Then naturally a question of irreducibility of polynomial over a field $\mathbb{F}_q$ arises and then one can think of the quotient ring $\mathbb{F}_q[x]/(f(x))$. The factorization of a polynomial $f(x)$ over $\mathbb{F}_q$ is ingeneral a difficult problems. But the polynomial $x^n - 1$ can be fcatorized easily over a field $\mathbb{F}_q$. And the ideal generated by irreducible factors of $x^n - 1$ leads to the class of cyclic codes.

But, in general for a non zero constant $c \neq 1$, the factorization of $x^n - c$ leads a another very beautful class of cyclic codes called constacylic codes. These codes have become interest of reserach recnetly. Various rereachres have contibuted in the study of these consta cyclic codes. For example one can refer [11, 13].

Recently Ryan, Tsfasman, Nogin, Ghorpade, Lachuad, Patil, Pillai [14, 16, 17, 18] have developed a elegant connection of Algebraic geomety to coding theory. This connection has been useful for both direction of reserach. That is. some results in algebraic geometry have been proved through the study of codes associated to different algebraic affine and projective varieties over a finite field.

2. **Aim and Objective of Research:** The main objective of my research during Ph.D. is to work on certain problems associated to codes over finite fields, finite rings:

   (i) We will investigate and expand some properties of algebraic codes.

   (ii) We will study cyclic, constacyclic, negacyclic codes and their duals over finite fields and finite rings.

   (iii) We will study concatanation of some available codes over finite fileds and finte rings and their extensions.

   (iv) We will explore the algebraic geometric codes and open problems in this area of research.

3. **Methodology to be adopted:** My area of research is theoretical in nature. Mostly, I will be referring the text books and research papers of various researchers who have developed this area of research. I would also like to consult with my thesis supervisor time to time to discuss the doubts. I would also like to participate in the schools, seminars, workshops in my area of research, which will help me to strengthen my knowledge in my field of research.

4. **Importance of study:** The area of my research is highly applicable in coding theory. Coding theory has its origins in the engineering problem of effective electronic communication where the alphabet is generally the binary field. Since its inception, it has grown as a branch of mathematics, and has since been expanded to consider any finite fields, and later also finite rings, as its alphabet. This proposal will presents a broad view of the subject and relates major results by ring theory.

5. **Proposed Work Plan:** Following is the Year-wise plan of work and target to be achieved during my research period:

   Year 1:
   Course work and reading : I will complete the course work and other academic formalities

declared by SRTMU Nanded in the first semester. Then after, I would like to read the following text books to develop necessary background for my research:

(i) R. Lidl and H. Niederreiter, Introduction to Finite Fields and Their Applications, rev. ed. Cambridge, England: Cambridge University Press, (1994).

(ii) F. J. MacWilliams and N. J. A. Sloane, *The Theorey of Error Correcting Codes*, North Holland, Amsterdam, 1977.

Year 2:
I would like to read the research papers, text books, and would like to complete research related literature survey and decide the problem for my PhD thesis in consultation with my thesis supervisor. I would also like to participate in various national and international workshops, schools and conferences to get the broader view and to develop academic relations with other reserachers who are working in my field.

Year 3: I will focus on my research problem and would like to learn various techniques and methods by the other researchers on my area of research.

Year 4: I will try to solve my thesis problem and try to have my publications related to my work.

Year 5: I will try to write my thesis and submit to university for the award of PhD.

References

[1] T. Steven, Dougherty, Algebraic coding theory over finite commutative Rings, Springer Briefs in Mathematics, (2012).

[2] I. Blak, Codes over certain rings. Inf. control, 29(4), 295-300 (1975).

[3] R. Lidl and H. Niederreiter, Introduction to Finite Fields and Their Applications, rev. ed. Cambridge, England: Cambridge University Press, (1994).

[4] R. Hamming, Error detecting and error correcting codes. Bell Syst. Tech. J. 29, 147-160 (1950).

[5] C. Shannon, A mathematical theory of communication. Bell Syst. Techn. J. 27 (1948).

[6] S.T. Dougherty, J. Kim, P. Sole, Open problems in coding theory, Contemp. Math. 634, 79-99 (2015).

[7] S.T. Dougherty, A. Kaya, E. Salturk, Cyclic codes over local frobenius rings of order 16. Adv. Math. Comm. 11(1), 99-114 (2017).

[8] M. Shi, A. Alahmadi, and P. Sole,Codes and Rings: Theory and Practice, Academic Press (2017).

[9] K. Guenda, New MDS self-dual codes over finite fields, Des. Codes Cryptogr., 62, 31-42 (2012).

[10] B. Yildiz and S. Karadeniz, Cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, Des. Codes Cryptogr., 58, 221-234 (2011).

[11] S. Zhu and L. Wang, A class of constacyclic codes over $\mathbb{F}_p + u\mathbb{F}_p$ and its Gray image, Discrete Mathematics, 311, 2677-2682 (2011).

[12] R. T. Chien, Cyclic Decoding Procedure for the Bose-Chaudhuri-Hocquenghem Codes, EEE Trans. on Inf. Th., vol. 10, p. 357-363, 1964.

[13] T. Abualrub and I. Siap, Constacyclic codes over F2 + uF2, J. Franklin Inst., 346, 520529, 2009

[14] C. T. Ryan, *Projective codes based on Grassmann varieties* , Congr. Numer. 57, 273-279, 1987

[15] F. J. MacWilliams and N. J. A. Sloane, *The Theorey of Error Correcting Codes*, North Holland, Amsterdam, 1977.

[16] M. A. Tsfasman and S. G. Vlăduţ, *Algebraic Geometric Codes*, Kluwer, Amsterdam, 1991.

[17] S. R. Ghorpade and G. Lachaud, *Hyperplane sections of Grassmannians and the number of MDS linear codes*, Finite Fields Appl. vol. 7, 468-506, 2001.

[18] S. R. Ghorpade, A. R. Patil, H. K. Pillai, *Decomposable subspaces, linear Sections of Grassmann varieties, and higher weights of Grassmann codes*, Finite Fields Appl.15, 54-68, 2009.

Mrs. Somaiyah A.A. Abdulsattart
Research Student

Dr. Arunkumar R. Patil
Research Guide

DR.ARUNKUMAR R. PATIL
Associate Professor
Dept. of Mathematics
SGGS Institute of Engg.& Tech.
Vishnupuri,Nanded - 431606.